Abstract

An exponentiation operation or other computational task associated with a cryptographic protocol is performed in a secure distributed manner using multiple machines, e.g., a client device and multiple servers of a computer network. The computational task is transformed by an originator machine before being sent to one or more external servers for execution. The transformation may include replication and dependency operations to provide robustness to errors in the computations performed by the external servers, and blinding and permutation operations to provide privacy for secret information associated with the computational task. The transformed computational task is executed by the one or more external servers, and the results of the transformed computational task are transmitted back to the originator machine. The originator machine transforms the results of the transformed computational task in a manner which permits verification that the one or more results are appropriate results for a given input. Advantageously, the invention can operate with arbitrary inputs, and provides improved computational efficiency relative to conventional techniques for both small and large batches of cryptography-related computations.